Daffodil International University

Faculty of Science & Information Technology
Department of Computer Science & Engineering
Final Semester Examination, Fall 2024
Course Code: CSE423, Course Title: Information Security
Level: 4 Term: 1, 2 Batch: 58, 59, 60

Time: 2 Hrs **Marks: 40**

Answer ALL Questions

[The figures in the right margin indicate the full marks and corresponding course outcomes. All portions of each question must be answered sequentially.]

1.	a)	A company discovers a breach in its customer database after an employee detects suspicious access attempts from an unusual IP address. The company has a pre-established incident response plan and trained staff to handle such situations. The incident is reported and documented as a high-priority case. The response team takes steps to manage the incident, including isolating affected servers, notifying stakeholders, analyzing logs, eliminating malicious software, restoring systems. After resolving the issue, the team reviews the incident, documents findings, revises policies, and implements measures to prevent future attacks. **Analyze** the scenario and relate each action to its corresponding stage in the Incident Handling and Response (IH&R) process.	[5]	CO1
	b)	A cybersecurity team is tasked with enhancing the security posture of an organization that frequently faces phishing attempts and malware attacks. **Apply** your knowledge of AI and ML to describe five key applications of these technologies that could be implemented to strengthen the organization's defense.	[5]	
	c)	Today, blockchain is widely recognized as a revolutionary technology for securing digital transactions and managing decentralized data systems. It is transforming industries with its innovative approach to data integrity and security. **Illustrate** the key features of blockchain technology with detailed explanations for each feature that make it a reliable and transformative tool in modern systems.	[5]	
2.	a)	A company is experiencing frequent cyber threats, including unauthorized access attempts and malware attacks. Despite having a firewall and antivirus, the IT team struggles to detect and prevent advanced threats. The company is planning to enhance its security infrastructure by implementing measures to identify potential threats, prevent unauthorized access, and set up decoys to mislead attackers. Now **break down** the roles of these strategies in the company's overall security management.	[6]	CO2

	b)	**Apply** your understanding of symmetric encryption, asymmetric encryption, and hashing techniques to demonstrate how they contribute to achieving the key principles of the CIA triad and discuss their roles in securing a user's personal data.	**[4]**	
	c)	DIU is evaluating the risks to its online resources by assessing the potential impact of security breaches. The Teacher Portal and MMS system are both identified as having a high impact if compromised. The SmartEdu and Student Portal platforms are assessed with a medium impact in the event of an attack. Lastly, the BLC system is expected to have minimal impact if targeted. This analysis highlights the varying levels of impact across the organization's online assets. Additionally, the likelihood of attacks on each asset is measured as shown in the table below. **Assets** / **Likelihood** Teacher Portal / 1 SmartEdu / 0.5 Student Portal / 0.5 MMS / 1 BLC / 0.1 Based on the provided data, **calculate** the risk level for each asset and the overall risk rating. This will help prioritize security efforts and focus on the most vulnerable assets of the organization.	**[5]**	
3.		A software development company has created a revolutionary algorithm that processes large amounts of data faster and more efficiently than ever before. This innovation could transform industries like healthcare and finance to a great extent, giving the company a major advantage over competitors. However, others might try to copy it. Discuss the different ways the company can protect its algorithm using intellectual properties. Now **apply** your understanding to choose which option would be the best to keep their algorithm safe and help the company stay ahead in the market.	**[4]**	**CO3**
4.		**Demonstrate** the legal penalties outlined in Sections 18, 20, and 32 of the Digital Security Act 2023 for individuals who commit offenses such as unauthorized access, source code modification, or hacking and how these provisions help mitigate cybercrimes?	**[6]**	**CO3**